

ANNOTATIE

G.D. t. the Commissioner of the Garda Síochána e.a. (HvJ EU, C-140/20) – Een nieuwe episode in de dataretentiejurisprudentie

R.H.T. Jansen en R.M. te Molder

Annotatie bij Hof van Justitie van de Europese Unie, 05-04-2022, ECLI:EU:C:2022:258 (EHRC-2022-0117)

Inleiding

1. Dataretentievraagstukken veroorzaken een gestage jurisprudentiestroom.[1] Onlangs heeft het Hof van Justitie van de EU (HvJ EU) de jurisprudentiële lijnen uit de richtinggevende arresten *La Quadrature du Net*[2] en *Prokuratuur*[3] nog eens bestendigd. In de ogen van advocaat-generaal Campos Sánchez-Bordona was de rechtsgang zelfs onnodig. Hij vond dat het HvJ EU de hier aan de orde zijnde vragen reeds ‘afdoende’ had beantwoord.[4] Het Ierse *Supreme Court* had weliswaar van de eerdere uitspraken kennisgenomen, maar zich daarover ‘nogal laconiek’ uitgelaten en toch aangedrongen op een nieuwe prejudiciële beslissing, aldus de A-G.[5] De vraag is of hij met die stellingname niet te kort door de bocht is gegaan. Weliswaar waren de door het Ierse Hof geformuleerde vragen niet nieuw, het onderhavige arrest biedt op een onderdeel wel degelijk een nadere precisering van bestaande jurisprudentiële lijnen. De uitspraak biedt evenwel geen blauwdrukken voor wetgeving en roept dus, net als de eerdere uitspraken, vragen op over de implementatie ervan in de Nederlandse context.[6]

2. In deze annotatie staan twee aspecten centraal. Het eerste is hoe de Nederlandse wetgever met inachtneming van de criteria van het HvJ EU een bewaarplicht kan vormgeven. Nederland kent momenteel geen bewaarplicht en de ontwikkelingen op dit gebied liggen al geruime tijd

stil. Het tweede is of de door het HvJ EU geprefereerde onafhankelijke *ex ante*- toetsing ook buiten de context van het vorderen van verkeers- en locatiegegevens uitwerking zou moeten krijgen. De opzet is als volgt. Eerst schetsen wij kort de zaak alsmede de belangrijkste uitgangspunten die gelden op het gebied van het bewaren en vorderen van verkeers- en locatiegegevens, en daarna behandelen wij de genoemde aspecten.[7]

Zaakschets

3. In maart 2015 is G.D. veroordeeld tot een levenslange gevangenisstraf wegens moord op een Ierse vrouw. In beroep heeft hij onder meer aangevoerd dat de eerstelijnsrechter ten onrechte verkeers- en locatiegegevens heeft toegelaten als bewijs. Om in de strafprocedure de ontvankelijkheid van dat bewijsmateriaal te kunnen betwisten, is G.D. gelijktijdig bij de *High Court* een civiele procedure gestart. Via civiele weg vocht hij de geldigheid aan van enkele bepalingen van een Ierse dataretentiewet uit 2011. Op grond van die wet moeten communicatieaanbieders metagegevens over communicatie bewaren, zodat de autoriteiten de gegevens later kunnen vorderen en raadplegen voor het opsporen, onderzoek en vervolgen van strafbare feiten.[8] In casu ging het vooral om de Ierse politie, de *An Garda Síochána*. G.D. vorderde ongeldigheidsverklaring van de bepalingen, zodat hij in het strafrechtelijke hoger beroep kon betogen dat de metagegevens ontoelaatbaar zijn als bewijs. Zijn betoog behelsde, kort samengevat, het volgende. De bestreden bepalingen zijn in strijd met de rechten die G.D. aan het Unierecht ontleent. Preciezer: de Ierse wet zou onverenigbaar zijn met artikel 15 lid 1 van Richtlijn 2022/58/EG gelezen in het licht van de artikelen 7 en 8 alsmede artikel 52 lid 1 van het Europese Grondrechtenhandvest, omdat die wet slechts minimale waarborgen bevatte en niet nauwkeurig vastlegde in welke omstandigheden en onder welke voorwaarden autoriteiten toegang tot metagegevens mogen vorderen.

4. Het *High Court* stelde G.D. op 6 december 2018 in het gelijk. De wettelijke bepalingen zouden inderdaad in strijd zijn met het Unierecht. De verweerders – de *Commssioner of the Garda Síochána*, het Ministerie voor Communicatie en de *Attorney General* – stelden zich op een ander standpunt. De Staat ging dan ook tegen de beslissing in beroep bij het *Supreme Court*, de hoogste rechterlijke instantie van Ierland. Het *Supreme Court* formuleerde in de beroepsprocedure een zestal vragen en diende op 25 maart 2020 het verzoek in tot een prejudiciële beslissing. Het wenste met name duidelijkheid te verkrijgen over de vereisten die het Unierecht stelt aan het bewaren van metadata ter bestrijding van ernstige strafbare feiten en over de noodzakelijke garanties bij de toegang tot die gegevens. Voorts vroeg het zich af wat de omgang en de gevolgen zijn indien de bepalingen uit de Ierse wet van 2011 onverenigbaar zijn met het Unierecht. Problematisch was namelijk dat die wet diende ter omzetting van Richtlijn 2006/24/EG, die het HvJ EU in *Digital Rights Ireland e.a.* juist ongeldig had verklaard.[9] Ter overweging gaf het *Supreme Court* nog mee dat, als het ondanks solide

toegangsregelingen niet zou zijn toegestaan om metagegevens universeel te bewaren, de plegers van verschillende categorieën strafbare feiten niet zouden kunnen worden opgespoord of vervolgd.

Bevestiging en precisering van algemene uitgangspunten

5. Zoals wij al aanstipten, bevestigt het HvJ EU in deze uitspraak bestaande jurisprudentiële lijnen. Ten eerste neemt het wederom als vertrekpunt dat een algemene en ongedifferentieerde bewaarplicht van verkeers- en locatiegegevens alleen is toegestaan indien sprake is van een reële, actuele of voorzienbare dreiging voor de nationale veiligheid.[10] Ter bestrijding van (zeer) ernstige criminaliteit is zo'n bewaarplicht niet toegestaan. Een bewaarplicht voor ernstige criminaliteit is slechts toelaatbaar als de 'categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, [is limited; onze toevoeging] to what is strictly necessary'. [11] Een bewaarplicht voor ernstige criminaliteit moet dus zijn beperkt, bijvoorbeeld naar kring van personen, tijdsperiode en/of geografische zone.

6. Wel nieuw ten opzichte van eerdere jurisprudentie is, dat het HvJ EU de wijze waarop invulling kan worden gegeven aan een bewaarplicht concretiseert. Voor wat betreft de kring van personen geldt dat lidstaten in het bijzonder bewaringsmaatregelen kunnen treffen voor personen naar wie een onderzoek loopt; jegens wie andere onderzoeksbevoegdheden worden ingezet alsmede personen die een strafblad hebben waaruit blijkt dat zij reeds veroordeeld zijn voor een ernstig strafbaar feit met een mogelijk groot recidiverisico. Voor de geografische criteria geldt dat het gemiddelde criminaliteitscijfer in een bepaalde zone kan dienen als aanknopingspunt voor het afbakenen van een nationale bewaarplicht van verkeers- en locatiegegevens. Te betwijfelen valt evenwel of deze criteria werkbaar zijn in de toepassingspraktijk. Wij gaan daar zo nader op in.

7. Een tweede vraag die het HvJ EU in de onderhavige uitspraak wil ophelderen, betreft de vraag of gegevens die op basis van artikel 15 lid 1 Richtlijn 2002/58 met het oog op de nationale veiligheid zijn bewaard vervolgens mogen worden gevorderd door de strafvorderlijke autoriteiten voor de bestrijding van (zeer) ernstige criminaliteit. In het *La Quadrature*-arrest heeft het HvJ EU deze vraag niet expliciet beantwoord,[12] hetgeen door de Deense overheid, die als interveniërende partij optrad, is aangegrepen om te betogen dat zoiets mogelijk zou moeten zijn.[13] Het HvJ EU denkt daar anders over. Gegevens die zijn bewaard op basis van een maatregel in de zin van artikel 15 lid 1 Richtlijn 2002/58 mogen in beginsel enkel worden gevorderd voor hetzelfde doel als waarvoor de gegevens zijn bewaard. Dit is slechts anders 'wanneer de met de toegang nagestreefde doelstelling belangrijker is dan die welke de bewaring rechtvaardigde'. [14]

8. Op deze manier handhaaft het HvJ EU een strikte scheiding tussen de domeinen ‘nationale veiligheid’ en ‘strafrecht’.[15] Als gegevens met het oog op de nationale veiligheid zijn bewaard, dan mogen die gegevens ook enkel met het oog op de nationale veiligheid worden gevorderd. Opmerking verdient hier wel dat de voorgaande overwegingen van het HvJ EU steeds betrekking hebben op de situaties waarin gegevens zijn bewaard op basis van art. 15 lid 1 Richtlijn 2002/58. De vraag of de autoriteiten gegevens kunnen vorderen die voor bedrijfsdoeleinden – bijvoorbeeld facturering – zijn bewaard, blijft dus nog steeds onbeantwoord.[16] De redeneringen in het onderhavige arrest, net als die in *La Quadrature*, lijken er niettemin op te wijzen dat het vorderen van gegevens die bewaard zijn voor factureringsdoeleinden wel kunnen worden gevorderd voor de bestrijding van ernstige criminaliteit, omdat dit laatste doel zwaarder weegt dan het eerste.[17]

9. Voorts bevestigt het HvJ EU het belang van onafhankelijke toetsing voorafgaand aan het vorderen van verkeers- en locatiegegevens.[18] De Ierse rechter vroeg in hoeverre bij de beoordeling van de vraag of de rechter of een andere bestuurlijke entiteit onafhankelijk is, rekening kan worden gehouden met rechterlijke of andersoortige toetsing achteraf. Ter beantwoording van deze vraag wijst het HvJ EU vooral naar het *Prokuratuur*-arrest, waarin het heeft uiteengezet dat voorafgaande toetsing door een rechter of een andere onafhankelijke entiteit het uitgangspunt is. Alleen in uitzonderlijke gevallen kan hiervan af worden gezien.[19] In casu betekent dit dat *ex ante*-toetsing door een politiefunctionaris die een zekere mate van autonomie bezit en achteraf door een rechter kan worden getoetst in strijd is met het Grondrechtenhandvest. Gelet op eerdere rechtspraak en het belang dat daarin is toegekend aan voorafgaande onafhankelijke toetsing is deze uitkomst niet opvallend.

Bewaarplicht naar nationaal recht

10. Nederland kent momenteel geen bewaarplicht in de zin van art. 15 lid 1 Richtlijn 2002/58, op basis waarvan communicatieaanbieders worden verplicht verkeers- en locatiegegevens te bewaren met het oog op de in dit artikel genoemde belangen (nationale veiligheid, bestrijding van criminaliteit, etc.).[20] Verkeers- en locatiegegevens worden in Nederland dus enkel bewaard op basis van andere (commerciële) gronden, zoals facturering. Mocht Nederland een wettelijke regeling willen treffen, dan is het onderhavige arrest van belang. Tegelijkertijd is echter de vraag in hoeverre de Nederlandse wetgever kan varen op de door het HvJ EU aangebrachte preciseringen.[21] Dat geldt in het bijzonder voor het gemiddelde criminaliteitscijfer in een bepaalde geografische zone dat volgens het HvJ EU kan worden gebruikt om een bewaarplicht vorm te geven. Verschillende problemen doen zich voor met betrekking tot dit criterium.

11. Hoewel criminaliteitscijfers op het eerste gezicht wellicht ‘objectief’ zijn, valt te betwijfelen

of dat altijd het geval is. Zulke cijfers zijn niet zelden gekleurd. Er sluipt al snel een bias in. Als de politie haar capaciteit vooral inzet om bepaalde strafbare feiten – bijvoorbeeld de in het straatbeeld zichtbare criminaliteit – op te sporen, is de kans groter dat alleen deze strafbare feiten worden geconstateerd, met als gevolg dat de cijfers herbevestigend werken. Ook ligt discriminatie op de loer als blijkt dat de criminaliteitscijfers bias bevatten ten opzichte van minderheden.

12. Voorts doen zich ook met betrekking tot het criterium als zodanig allerlei vragen voor. Uit het criminaliteitscijfer moet blijken dat het gaat om een plek waar zware strafbare feiten worden gepleegd of op zijn minst om een plek waar een verhoogd risico op zware criminaliteit bestaat. Omdat het HvJ EU verder in het midden laat in welke gevallen lidstaten criminaliteitscijfers kunnen gebruiken om communicatieaanbieders te verplichten verkeers- en locatiegegevens te bewaren, is onduidelijk hoe dit alles in de praktijk precies moet worden gerealiseerd. Aangenomen dat alleen een (tijdelijke) stijging van de criminaliteitscijfers in een bepaalde locatie aanleiding kunnen geven tot een bewaarplicht: in welke mate is voor het opleggen van zo'n bewaarplicht een stijging van het gemiddeld criminaliteitscijfer nodig en hoe moet die stijging precies worden vastgesteld? Is daarvoor vereist om een vergelijking te maken met het verleden, of met andere gebieden? Ook verder blijft veel onduidelijk. Zo is niet duidelijk welk gebied onder zo'n bewaarplicht mag vallen. Een algemene en ongedifferentieerde bewaarplicht is niet toegestaan, maar de vraag is hoe het zit met bijvoorbeeld een provincie, een stad, een wijk of een buurt.

13. Ook met betrekking tot het strafblad als criterium om een bewaarplicht vorm te geven, valt de vraag te stellen of dit wel, zoals het HvJ EU het doet voorkomen, zo'n 'objectief' criterium is. Personen met een strafblad waaruit een verhoogd risico op recidive blijkt, worden immers gelijkgesteld met personen ten aanzien van wie uit feiten en omstandigheden blijkt dat zij als verdachte kunnen worden aangemerkt. De vraag is of deze gelijkstelling is te rechtvaardigen.

Ex ante toetsing naar nationaal recht

14. Met het oog op de normering van de digitale opsporing in het (gemoderniseerde) Wetboek van Strafvordering rijzen vragen over de *ex ante*-toetsing waar het HvJ EU ook in onderhavige uitspraak veel belang aan toekent. Een belangrijke vraag is, of de door het HvJ EU vereiste *ex ante*-toetsing ook voor andere bevoegdheden dan het vorderen van verkeers- en locatiegegevens zou moeten gelden waarmee een vergelijkbare of ernstigere inbreuk op het recht op privacy wordt gemaakt.[22] Nadere doordenking van de (praktische) consequenties van een dergelijke wijziging is, in het bijzonder in het kader van de modernisering van het Wetboek van Strafvordering, wenselijk. Op het eerste oog lijkt het aantrekkelijk om *ex ante*-toetsing vaker dan thans het geval is door een rechter-commissaris in plaats van een officier

van justitie uit te voeren. Weliswaar is een rechter-commissaris onafhankelijker dan een officier van justitie, maar de vraag naar toetsing verdient meer fundamentele aandacht.

15. *Ex ante*-toetsing is vaak statisch van aard en daarom vooral geschikt in situaties waarin de verschillende belangen tegen elkaar kunnen worden gewogen nog vóórdat een bevoegdheid wordt ingezet. Te betwijfelen valt of deze vorm van toetsing adequaat is als het gaat om digitale opsporingsbevoegdheden. Kenmerkend voor zulke bevoegdheden is juist het dynamische karakter, waarbij geldt dat in het bijzonder de ernst van de inbreuk op het recht op privacy zich niet gemakkelijk vooraf laat bepalen; de omstandigheden van het geval zijn bepalend. Toezicht achteraf – en wellicht: tijdens uitoefening van de bevoegdheid – lijkt in dit verband meer soelaas te kunnen bieden.[23] Momenteel speelt een soortgelijke discussie bij de normering van de AIVD en de MIVD. Daar is de tendens intussen dat het zwaartepunt moet worden verlegd van de *ex ante*-toets naar *ex durante*- en *ex post*-toezicht, zodat het toezicht beter aansluit bij het dynamische karakter van een bevoegdheidsuitoefening in het digitale domein.[24]

Conclusie

16. Al met al is de toegevoegde waarde van deze uitspraak ten opzichte van bestaande dataretentiejurisprudentie beperkt. Het betreft hier immers een bestending van bestaande jurisprudentiële lijnen. De A-G had daarvoor al gewaarschuwd. Interessant is vooral dat het HvJ EU nieuwe criteria aanreikt aan de hand waarvan een nationale bewaarplicht kan worden afgebakend, maar dat deze criteria vooral vragen oproepen. Voorts is interessant dat het HvJ EU hier nog eens onderstreept dat voor de toegang tot de bewaarde verkeers- en locatiegegevens een voorafgaande toetsing door een rechterlijke instantie of door een onafhankelijke administratieve entiteit nodig is. De vraag is evenwel hoe dit alles in de praktijk haalbaar en werkzaam is.

R.H.T. Jansen

Rowin Jansen is als docent en promovendus Algemene rechtswetenschap verbonden aan het Onderzoekcentrum voor Staat en Recht alsook aan de Interdisciplinary Hub for Digitalization and Society van de Radboud Universiteit.

R.M. te Molder

Ruben te Molder is als promovendus Straf(proces)recht verbonden het Onderzoekcentrum voor Staat en Recht alsook aan de Interdisciplinary Hub for Digitalization and Society van de Radboud Universiteit.

[1] Zie onder meer HvJ EU 2 oktober 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, «EHRC» 2019/18 m.nt. Van der Sloot; *La Quadrature du Net*, HvJ EU 6 oktober 2020, C-511/18, ECLI:EU:C:2020:791, *EHRC Updates* 2020-0253 m.nt. Schroers; HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152 (*Prokuratuur*), *EHRC Updates* 2021-0088 m.nt. Van Toor en recenter HvJ EU 20 september, C-793/19 en C-974/19, ECLI:EU:C:2022:702 (*Spacenet*), *EHRC Updates* 2022-0242.

[2] *La Quadrature du Net*, HvJ EU 6 oktober 2020, C-511/18, ECLI:EU:C:2020:791, *EHRC Updates* 2020-0253 m.nt. Schroers.

[3] *Prokuratuur*, HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, *EHRC Updates* 2021-0088 m.nt. Van Toor

[4] Conclusie AG, par. 24.

[5] Conclusie AG, par. 26.

[6] Zie in dit verband ook de cassatie in het belang der wet naar aanleiding van *Prokuratuur*: HR 5 april 2022, ECLI:NL:HR:2022:475.

[7] Wij gaan hier niet in op het bewaren en vorderen van identificerende gegevens alsmede IP-adressen. Zie daarover *La Quadrature du Net*, HvJ EU 6 oktober 2020, C-511/18, ECLI:EU:C:2020:791, par. 152-159, *EHRC Updates* 2020-0253 m.nt. Schroers.

[8] The Communications (Retention of Data) Act 2011. De wet is inmiddels geamendeerd.

[9] *Digital Rights Ireland*, HvJ EU 8 april 2014, C-293/12, ECLI:EU:C:2014:238, «EHRC» 2014/140 m.nt. Koning.

[10] *G.D. t. the Commissioner of the Garda Síochána e.a.*, par. 58.

[11] *La Quadrature du Net*, HvJ EU 6 oktober 2020, C-511/18, ECLI:EU:C:2020:791, par. 147, *EHRC Updates* 2020-0253 m.nt. Schroers.

[12] Sajfert wees in een blog reeds op de onduidelijkheid die het HvJ EU op dit punt liet bestaan. <https://europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/>. Zie ook R. de Keersmaecker & C. van de Heyning, 'De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga', *Tijdschrift voor Strafrecht* 2021, afl. 4, p. 185.

[13] *G.D. t. the Commissioner of the Garda Síochána e.a.* par. 96.

[14] *G.D. t. the Commissioner of the Garda Síochána e.a.* par. 98. Zie ook *La Quadrature du Net*, par. 165-165.

[15] *G.D. t. the Commissioner of the Garda Síochána e.a.*, par. 53, 56-57, 59 en 99. Zie hierover M. Tzanou & S. Karyda, 'Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga?', *European Public Law* 2022, afl. 1, p. 130-134.

[16] Deze vraag heeft de Hoge Raad in ECLI:NL:HR:2022:475 ook niet expliciet gesteld aan het HvJ EU. Wel heeft de Hoge Raad de vraag gesteld of het toegang verlenen tot gegevens die op andere gronden worden bewaard dan de in art. 15 lid 1 Richtlijn 2002/58/EG genoemde gronden onder de werking van de Richtlijn 2002/58/EG vallen.

[17] Vgl. Keersmaecker & Van de Heyning 2021, p. 185-186.

[18] Zie uitgebreid G.P. Sholeh, 'De betekenis van het Prokuratuur-arrest: digitale opsporing en privacy onder de loep', *DD* 2022, afl. 3, p. 227-247.

[19] *Prokuratuur*, HvJEU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, *EHRC Updates* 2021-0088 m.nt. Van Toor.

[20] De laatste ontwikkeling op dit terrein betreft een brief van de Minister van Justitie en Veiligheid van 25 september 2018, *Kamerstukken II* 2018/19, 34537, nr. 8 waarin hij aankondigt een nieuw onderzoek te laten uitvoeren. Dit onderzoek is inmiddels uitgevoerd (T. van der Vorst, e.a., *Mogelijkheden voor identificatie op internet op basis van IP-adres*, Den Haag: 2019). Een nieuw voorstel is nog niet ingediend.

[21] Zie over de moeilijkheden hierover uitgebreider: R.M. te Molder, 'Het bewaren en vorderen van metagegevens ten behoeve van de opsporing: meer duidelijkheid van het HvJ EU gewenst', *DD* 2021, afl. 9, p. 860-863.

[22] Vgl. in dit verband ook het advies van de Raad van State over de modernisering van het Wetboek van Strafvordering (d.d. 16 mei 2022), in het bijzonder in Deeladvies C over de opsporing, p. 135-136, en R.J. Verbeek, 'De Innovatiewet Strafvordering: het eerste spoor van het nieuwe Wetboek van Strafvordering', *Ars Aequi* 2022, afl. 10, p. 802-805

[23] Vgl. in dit verband M.I. Fedorova e.a., *Strafvorderlijke gegevensverwerking. Een verkennende studie naar de relevante gezichtspunten bij de normering van persoonsgegevens voor strafvorderlijke doeleinden*, WODC, Nijmegen: Radboud University Press 2022, p. 115 en 171.

[24] Commissie-Jones-Bos, *Evaluatie 2020. Wet op de inlichtingen- en veiligheidsdiensten 2017*, Den Haag 2021, m.n. hoofdstuk 9. Vgl. J.J. Oerlemans & Q.A.M. Eijkman, 'Evaluatie Wiv 2017:

betere uitvoerbaarheid, ten koste van privacy?', *Tijdschrift voor Internetrecht* 2021, afl. 3, 95-101;
R.H.T. Jansen, 'Van accentverschuiving naar stelselwijziging. Toezicht in het conceptvoorstel
Tijdelijke cyberwet voor de AIVD en de MIVD', *Nederlands Juristenblad* 2022, afl. 30, p. 2406-
2416.